[260] What is claimed is:

1. A method of secure communication between a resource-constrained device and remote network nodes over a network wherein the remote network nodes communicate with the resource-constrained device using un-modified network clients and servers and wherein the resource-constrained device has a central processing unit, a random access memory, a non-volatile memory, a read-only memory, and an input and output component, comprising:

using a physical link selected from one of several physical link methods;

executing on the resource-constrained device a communications module implementing networking protocols and one or more link layer communication protocols, operable to communicate with a host computer, operable to communicate with remote network nodes and operable to implement network security protocols thereby setting a security boundary inside the resource-constrained device;

implementing an execution model, wherein the communication module is driven by input events and by the applications and wherein the resource-constrained device uses at least one optimization technique selected from:

swapping data from the random access memory to the non-volatile memory;

swapping data from the non-volatile memory to the random access memory;

sharing data buffers between one or more communications protocol layers or security protocol layers;

executing on the host computer one or more link layer communication protocols operable to communicate with the resource-constrained device and operable to communicate with the remote network nodes; and

executing one or more secure network applications on the resource-constrained device wherein the network applications call upon the

communication module of the resource-constrained device to communicate with the remote network node wherein the secure network applications are securely accessible by the remote network nodes using un-modified network clients and servers.

2. The method of Claim 1 wherein the physical link is selected from the set including full-duplex serial connection, half-duplex serial connection, USB connection, contactless radio connection.

3. The method of Claim 2 wherein the physical link is a full-duplex serial connection using the serial peripheral interface protocol.

4. The method of Claim 1 further comprising connecting an interface device between the resource constrained device and the host computer using a physical link that is a serial connection having half-duplex between the resource constrained device and the interface device and full-duplex between the interface device and the host computer.

5. The method of Claim 4 further comprising operating the interface device to perform a bridging function between the half-duplex connection and the full-duplex connection.

6. The method of Claim 5 wherein the step of performing a bridging function further comprises providing at least one of function selected from:

enabling a resource constrained device operating in a command/response mode to communicate with network nodes as a peer;

enabling a resource constrained device operating in half-duplex communication mode to handle full-duplex communication traffic;

encapsulating upper layer protocol frames;

enabling transportation of upper layer protocol frames exceeding a frame size limit of the lower link layer; and

supporting multiple logical connections of upper layer protocols.

7. The method of Claim 4 of operating a software module on the interface device according to a finite state machine permitting the interface device to forward messages between the resource constrained device and the network wherein the interface device is in one of the at least one states permitting the resource constrained device to initiate and send messages.

8. The method of Claim 7 wherein the at least one state is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

9. The method of Claim 4 of operating a software module on the host computer according to a finite state machine having at least one state permitting the resource constrained device to transmit messages to the network wherein the software module is in one of the at least one states permitting the resource constrained device to initiate and send messages.

10. The method of Claim 9 wherein the at least one state is selected from a set of states corresponding to the interface device transmitting a Send, a Put, and a Poll command, respectively.

11. The method of Claim 9 comprising the step of operating the resource constrained device according to a finite state machine having at least one state in which the resource constrained device waits for a message from the host computer indicating that the resource constrained device may transmit a message.

12. The method of Claim 4 further comprising:

operating the resource constrained device according to a finite state machine whereby the resource constrained device uses the response status at the end of the response to the command sent by the host computer or an intermediate device to indicate that the resource constrained device wants to transmit information to the host computer or to the network.

13. The method of Claim 12 where in the step of operating the resource constrained device comprises operating the resource constrained device according to a finite state machine having at least one state in which the resource constrained device waits for a message indicating to the resource constrained device that the resource constrained device may transmit information to the host.

14. The method of Claim 13 further comprising operating the resource constrained device to transition among the states of the finite state machine.

15. The method of Claim 12 further comprising:

operating the host computer or an intermediate device connected between the host computer and the resource constrained device according to a finite state machine to transmit a polling message to the resource constrained device checking if the resource constrained device may want to transmit information to the host computer.

16. The method of Claim 15 where in the step of operating the host computer or intermediate device comprises operating the host computer or intermediate device according to a finite state machine having a Polling state in which the host computer or intermediate device polls the resource limited device, a Get-from-card state in which the host computer or intermediate device obtains packets of data from the resource constrained device, a Putting-to-card state in which the host computer or intermediate device transmits data to the resource constrained device, and a Checking RAS state in which the host computer or

intermediate device checks whether RAS has any data to transmit to the resource constrained device.

17. The method of Claim 16 further comprising operating the host computer or the intermediate device to transition among the states of the finite state machine.

18. The method of Claim 1 wherein the resource-constrained device is a smart card.

19. The method of Claim 1 wherein the resource-constrained device is a MultiMediaCard (MMC).

20. A resource-constrained device connected to a network and enabled to communicate with other nodes on the network, comprising:

at least one Internet application;

a communication module connected to the at least one Internet application and having:

a protocol module operable to implement TCP and IP protocols; and

a link layer module operable to implement the PPP protocol and a link layer protocol wherein the link layer protocol provides a bridge between Internet protocols and a lower level communications protocol.

21. The resource-constrained device of Claim 20, wherein the link layer module provides a function selected from:

enabling a resource constrained device operating in a command/response mode to communicate with network nodes as a peer;

enabling a resource constrained device operating in half-duplex communication mode to handle full-duplex communication traffic;

separating the upper layers and applications from the lower layer communication logic and implementation;

encapsulating upper layer protocol frames;

enabling transportation of upper layer protocol frames exceeding a frame size limit of the link layer module; and

supporting multiple logical connections of upper layer protocols.

22. The resource-constrained device of Claim 20, further comprising:

a buffer chain comprising a plurality of buffers and connected to the protocol module and the link layer module whereby the protocol module and the link layer module both access the buffers in the buffer chain.

23. The resource constrained device of Claim 22, wherein the buffer chain is a pbuf chain.

24. The resource-constrained device of Claim 22 wherein each buffer in the buffer chain may contain a payload and the buffers in a buffer chain is allocated from a pool of buffers and wherein the number of buffers in the pool and the size of each buffers payload are configurable according to the resource-constraints of the resource-constrained device.

25. The resource constrained device of Claim 22, wherein the payload size is 128 bytes and the number of buffers in the pool is four.

26. The resource-constrained device of Claim 20, wherein the link layer module comprises a PPP module for implementing the PPP protocol and a lower link layer protocol module for implementing a lower link layer protocol and further comprising an AHDLC module connected to the PPP module and the lower link layer protocol module and operable to receive PPP packets from the PPP module and to produce AHDLC frames, wherein the lower link layer protocol is below the PPP protocol in a protocol stack.

27. The resource-constrained device of Claim 26 wherein the AHDLC module is further operable to extract PPP data from AHDLC frames and to place the extracted PPP data onto the buffer chain and wherein the PPP module retrieves the PPP data from the buffer chain.

28. The resource-constrained device of Claim 27 wherein the AHDLC module places data into a current buffer and allocates a new current buffer from the buffer chain when the AHDLC module processes incoming data if the current buffer is full.

29. The resource-constrained device of Claim 26 wherein the PPP module consumes the buffer chain allocated by the AHDLC module.

30. The resource-constrained device of Claim 26 wherein the PPP module allocates buffers in the buffer chain for output processing.

31. The resource-constrained device of Claim 30 wherein the PPP module frees allocated buffers into the buffer pool as output packets are sent. The PPP module frees the allocated input buffers into the buffer pool if the data is intended for PPP module and not for upper layers or applications.

32. The resource-constrained device of Claim 20 wherein

the link-layer module comprises a PPP module for implementing the PPP protocol and a low link layer protocol module for implementing the low link-layer protocol; and wherein

the communications module further comprises:

a net server module connected to the at least one Internet application, an IP module, a TCP module and the PPP module wherein the net server module is operable to initialize the communications module and operable to determine a protocol type of incoming data and to demultiplex incoming data to one of the IP module,

the TCP module, and the PPP module in response to the detected protocol type;

an AHDLC module connected to the PPP module for processing PPP packets into AHDLC frames and processing AHDLC frames into PPP packets; and

a buffer chain of allocatable buffers connected to each of the PPP module, the IP module, TCP module and AHDLC module.

33. The resource-constrained device of Claim 32 wherein the AHDLC module is operable to allocate buffers in the buffer chain for storing AHDLC processed input data and wherein the PPP module, the IP module, and TCP module retrieves data from the buffers allocated by the AHDLC module.

34. The resource-constrained device of Claim 33 wherein the AHDLC module processes data stored in a data buffer and places the output sequentially into the same data buffer.

35. The resource-constrained device of Claim 20 wherein the resource-constrained device is a smart card.

36. The resource-constrained device of Claim 20 wherein the resource-constrained device is a MultiMediaCard (MMC).

37. A resource constrained device connected to a network and enabled to communicate with other nodes on a network having an architecture in which processing of application commands are separated from communications commands, comprising:

at least one Internet application; and

a communications module connected to the at least one Internet application and operable to implement at least one communications protocol independent from applications commands.

38. The resource-constrained device of Claim 37 wherein the communications module implements at least one communications protocol void of applications commands.

39. The resource-constrained device of Claim 37 wherein the communications module implements Internet protocols thereby providing the Internet application a communications and networking facility over which to transmit and receive data to and from Internet.

40. The resource-constrained device of Claim 37 further comprising a second Internet application connected to the communications module.

41. The resource-constrained device of Claim 26 wherein the link layer protocol module implements the Peer I/O protocol.

42. The resource-constrained device of Claim 22, wherein the TCP module demultiplexing places the buffer chain into the socket that corresponds to the destination of the data in the buffer chain.

43. The resource-constrained device of Claim 20, wherein the communications module, the link layer module, and the at least one Internet application execute in one thread.

44. The resource-constrained device of Claim 20, wherein the communications module executes in at least one thread and at least one Internet application execute in a second thread.

45. The resource-constrained device of Claim 44, wherein at least one Internet application executes in a first thread and at least one other of at least one Internet application executes in a second thread.

46. The resource-constrained device of Claim 37 wherein the resource-constrained device is a smart card.

47. The resource-constrained device of Claim 37 wherein the resource-constrained device is a MultiMediaCard (MMC).

48. A resource-constrained device connected to a network and enabled to communicate with other nodes on the network, comprising:

means for connecting the resource-constrained device to the network;

at least one application program executing on the resource-constrained device;

means for communicating with other nodes using a secure communications protocol stack including a link layer communications protocol, network communications protocol, and secure socket layer protocol;

wherein the at least one application program may communicate securely with a remote application program executing on another node by calling the means for communicating with other nodes.

49. A resource-constrained device for communicating with remote computers connected via a network wherein the resource constrains is a small random access memory, comprising:

connectors for connecting the resource-constrained device to the network;

a random access memory;

a reprogrammable non-volatile memory;

a central processing unit connected to the connectors, the random access memory, and the reprogrammable non-volatile memory,

wherein the reprogrammable non-volatile memory contains instructions for the central processing unit to cause the central processing unit to communicate with the remote computers on a peer-to-peer basis.

50. The resource-constrained device of Claim 49, wherein the connector communicates with devices external thereto using half-duplex and command/response communication protocol, wherein the instructions further comprise instructions to cause the central processing unit to:

implement a link-layer communication protocol stack that contains a specialized client-side link-layer communication protocol module operable to communicate with a corresponding server-side link layer communication protocol module wherein the link-layer communication protocol specifies communication of upper layer protocol frames using APDU wherein the server-side link layer communicates with at least one of the remote computers using full-duplex communication while communicating with the resource-constrained device using half-duplex thereby permitting full-duplex communication between the remote computer and the resource-constrained device.

51. The resource-constrained device of Claim 50 wherein the protocol frames are PPP frames.

52. The resource-constrained device of Claim 50, wherein the client-side link-layer communications protocol module is operable to receive messages larger than 256 bytes by receiving such messages on multiple APDUs.

53. The resource-constrained device of Claim 52, wherein the client-side link-layer communications protocol module operates according to a client-side finite state machine to receive sequences of APDUs making up higher-level protocol data frames larger than 256 bytes.

54. The resource-constrained device of Claim 53, wherein the client-side finite state machine comprises:

four states including an initial state, a waiting for upper layer instruction state, a ready write-waiting for message from server-side link-layer module, and ready read-waiting for message from server-side link-layer module;

five events including read instruction from upper layer protocol, write instruction to upper layer protocol, received poll command from server-side link-layer module, put command to server-side link-layer module, get command from server-side link-layer module; and

four actions including send a ready-write status to the server-side link-layer module including the length of the message to write, send a ready-read status to the server-side link-layer module, a get data from the server-side link-layer module, and a put data to the server-side link-layer module.

55. The resource-constrained device of Claim 49 wherein the resource-constraint is a random access memory of 20 kilobytes or less.

56. The resource-constrained device of Claim 49 wherein the reprogrammable non-volatile memory contains instructions for the central processing unit to cause the central processing unit to communicate in a secure manner using a transport layer security protocol with at least one of the remote computers on a peer-to-peer basis wherein the instructions to cause the central processing unit to communicate in a secure manner using a transport layer security protocol includes a server-side transport layer security protocol module (server-side TLS module) having instructions to perform authentication of the resource-constrained device and the remote computer, key exchange between the resource-constrained device and the remote computer, encryption of messages sent between the resource-constrained device and the remote computer, and

message digest of messages sent between the resource-constrained device and the remote computer.

57. The resource-constrained device of Claim 56 wherein the instructions to perform authentication of the resource-constrained device and the remote computer includes instructions to allocate memory to maintain a transport layer security protocol context state and to perform cryptographic operations by allocating required read access memory on a heap.

58. The resource-constrained device of Claim 56 wherein the server-side transport layer module includes instructions selected from the set including instructions to swap data from read-only memory into non-volatile memory in response to identifying a data block in read-only memory as stable and of sufficient size to justify swapping into non-volatile memory.

59. The resource-constrained device of Claim 58 further comprising instructions to cause the swapping of a data block from read-only memory into non-volatile memory to occur concurrently with decrypting a pre-master secret using an RSA private key.

60. The resource-constrained device of Claim 56 further comprising instructions to allocate a first buffer of random access memory; using the first buffer in a first context; re-using the first buffer in a second context wherein the first context and the second context are selected from the set of scenarios including (a) during handshake between the resource-constrained device and the remote computer, pre-master secret and the master secret, (b) during processing of client-key-exchange messages storing a value of an encrypted pre-master secret and incoming transport layer security protocol messages in the first buffer, and (c) using the first buffer for both DES encryption and DES decryption.